PN - DE19638623 A 19980326

PD - 1998-03-26

PR - DE19961038623 19960920

OPD - 1996-09-20

TI - Computer system with process for handling coded data

AB - The computer system has an interface 3 for receiving the coded data from a network 2. There is at least one output unit for outputting the public key data. The received data is handled by a central processor 4. Between the output unit and the central processor is a decryption unit 5. Use of the data is made by output units , such as a disc drive 6, a monitor 7 or a printer 8. For the printer and monitor the information is handled by the decoding units 5 and there is no requirement to return this data to the processor.

IN - HOGL CHRISTIAN (DE)

PA - HOGL CHRISTIAN (DE)

ICO - S06F1/00N7R ; S06F211/014B2

EC - H04L9/30 ; G06F1/00N7R

IC - H04L9/30 ; G06F12/14

TI - Computer system with process for handling coded data - has processor data decoded for output to specific peripherals

PR - DE19961038623 19960920

PN - DE19638623 A1 19980326 DW199818 H04L9/30 006pp

PA - (HOGL-I) HOGL C

IC - G06F12/14 ;H04L9/30

IN - HOGL C

AB - DE19638623 The computer system has an interface 3 for receiving the coded data from a network 2. There is at least one output unit for outputting the public key data. The received data is handled by a central processor 4. Between the output unit and the central processor is a decryption unit 5.

- Use of the data is made by output units , such as a disc drive 6, a monitor 7 or a printer 8. For the printer and monitor the information is handled by the decoding units 5 and there is no requirement to return this data to the processor.

- USE - For public key private key encrypted data transmission using computer systems.

- ADVANTAGE - Limits use of decoded data(Dwg. 1/1)

OPD - 1996-09-20

AN - 1998-194402 [18]

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 38 623 A 1**

(51) Int. Cl.[6]:
H 04 L 9/30
G 06 F 12/14

(21) Aktenzeichen: 196 38 623.3
(22) Anmeldetag: 20. 9. 96
(43) Offenlegungstag: 26. 3. 98

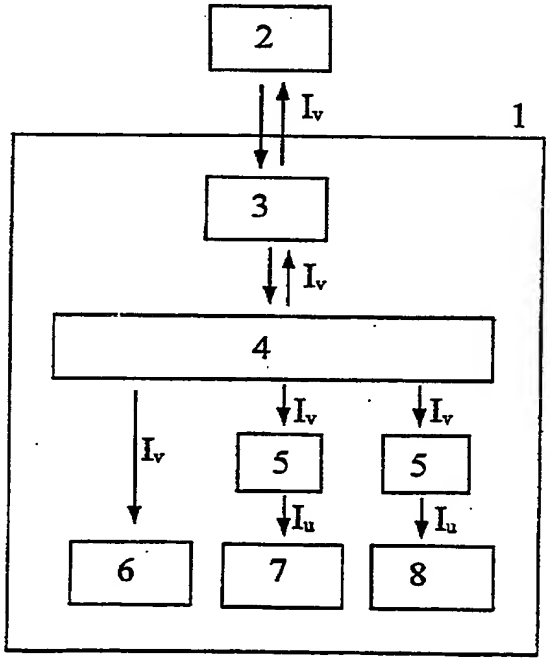
DE 196 38 623 A 1

(71) Anmelder:
Hogl, Christian, 80469 München, DE

(72) Erfinder:
gleich Anmelder

(54) Computersystem und Verfahren zur Ausgabe von verschlüsselten Daten

(57) Die Erfindung betrifft ein Computersystem 1 mit einer Schnittstelle 3 zum Empfang von verschlüsselten Daten, mindestens einer Ausgabeeinheit 7, 8 zur Ausgabe von unverschlüsselten Daten und einer Zentraleinheit 4 zum Empfang der Daten von der Schnittstelle 3 und zur Übermittlung auszugebender Daten an eine Ausgabeeinheit 7, 8. Das erfindungsgemäße Computersystem 1 zeichnet sich dadurch aus, daß zwischen der Zentraleinheit 4 und der Ausgabeeinheit 7, 8 eine Entschlüsselungseinheit 5 vorgesehen ist, welche die von der Zentraleinheit 4 kommenden Daten entschlüsselt und welche die entschlüsselten Daten nur an die zur Ausgabe von unverschlüsselten Daten vorgesehene/n Ausgabeeinheit/en 7, 8 übermittelt, wobei in dem Computersystem 1 keine Mittel zur Übermittlung der entschlüsselten Daten zurück an die Zentraleinheit 4 vorgesehen sind. Ferner betrifft die Erfindung ein Verfahren zur Ausgabe von verschlüsselten Daten, bei dem die verschlüsselten Daten über eine Schnittstelle 3 empfangen und an eine Zentraleinheit 4 übermittelt werden. Daraufhin werden die verschlüsselten Daten für die Ausgabe von der Zentraleinheit 4 an eine Entschlüsselungseinheit 5 übermittelt und von dieser entschlüsselt. Die entschlüsselten Daten werden von der Entschlüsselungseinheit 5 an eine bestimmte Ausgabeeinheit 7, 8 übermittelt und von dieser ausgegeben. Dabei ist es bei dem erfindungsgemäßen Verfahren nicht möglich, daß die entschlüsselten Daten zurück an die Zentraleinheit 4 übermittelt werden.



DE 196 38 623 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 01. 98 802 013/253 7/23

Beschreibung

Die vorliegende Erfindung bezieht sich auf ein Computersystem mit einer Schnittstelle zum Empfang von verschlüsselten Daten, mindestens einer Ausgabeeinheit zur Ausgabe von unverschlüsselten Daten und einer Zentraleinheit zum Empfang der Daten von der Schnittstelle und zur Übermittlung auszugebender Daten an eine Ausgabeeinheit nach dem Oberbegriff des Patentanspruches 1.

Ferner bezieht sich die Erfindung auf ein Verfahren zur Ausgabe von verschlüsselten Daten, bei dem die verschlüsselten Daten über eine Schnittstelle empfangen werden, die verschlüsselten Daten an eine Zentraleinheit übermittelt werden und die entschlüsselten Daten von einer Ausgabeeinheit ausgegeben werden nach dem Oberbegriff des Patentanspruchs 7.

In Netzwerken sind einzelne Computersysteme miteinander verbunden, die sich gegenseitig verschlüsselte Daten zusenden. Als Beispiel für ein solches Netzwerk ist das Internet zu nennen. Dort werden Informationen und audiovisuelle Signale verbreitet. Der Großteil des Angebotes sind unentgeltliche Informationen. Geldwerte Informationen werden bislang kaum angeboten, sondern bleiben auf herkömmliche Distributionskanäle beschrankt.

Dies hat unter anderem die folgenden drei Gründe:
Erstens sind Verfahren zur komfortablen Zahlungsabwicklung bislang noch nicht verbreitet. Zweitens gibt es bisher nur wenige Verfahren zur gesicherten Informationsübertragung. Sichere Verfahren basieren vorwiegend auf kryptographischen Public/Private-Key-Verfahren. Diese Verfahren zeichnen sich dadurch aus, daß jeder Teilnehmer am Informationsaustausch zwei Schlüssel besitzt:
Einen öffentlichen Schlüssel KÖ und einen privaten Schlüssel KP. Ein Zusammenhang zwischen beiden ist nicht ableitbar. Der öffentliche Schlüssel jedes Teilnehmers kann öffentlichen Verzeichnissen entnommen werden. Der private Schlüssel bleibt geheim und ist nur dem Teilnehmer selbst bekannt. Eine Information I, die mit dem öffentlichen Schlüssel KÖ verschlüsselt worden ist, kann nur mit dem privaten Schlüssel KP entschlüsselt werden und umgekehrt.

Public/Private-Key-Verfahren erfüllen zwei wichtige Funktionen:

a) Sie stellen sicher, daß über öffentliche Kanäle übertragene Informationen nur vom rechtmäßigen Empfänger genutzt werden können. Dazu verschlüsselt der Informationslieferant die Nachricht mit dem öffentlichen Schlüssel des rechtmäßigen Empfängers und versendet die verschlüsselte Nachricht über öffentliche Kanäle. Diese verschlüsselte Nachricht kann von jedem empfangen, aber nur vom rechtmäßigen Empfänger entschlüsselt und genutzt werden.
b) Sie stellen sicher, daß der Empfänger einer über öffentliche Kanäle übertragenen Information sicher gehen kann, daß diese tatsächlich vom rechtmäßigen Absender stammt.

Dazu verschlüsselt der Informationslieferant die Nachricht I mit seinem eigenen privaten Schlüssel und versendet die verschlüsselte Nachricht I über öffentliche Kanäle. Wenn bei einem Empfänger L der Entschlüsselungsversuch mit dem öffentlichen Schlüssel des Lieferanten Z gelingt, stellt dies sicher, daß die Nachricht I auch wirklich vom rechtmäßigen Lieferanten Z stammt.

Drittens können beim Empfänger in digitaler Form vorliegende Informationen von diesem mißbräuchlich weiterverbreitet werden. Dieses Problem ist wesentlich größer als bei nichtdigitalen Trägermedien (z. B. Papier), da eine digitale Weiterverbreitung schnell, verlustfrei und billig möglich ist.

Gemäß dem letztgenannten dritten Grund ergibt sich als wesentlicher Nachteil der herkömmlichen Informationsverbreitung über Netzwerke, daß die über das Netzwerk zur Verfügung gestellten Daten, selbst wenn sie verschlüsselt übermittelt werden, im Computersystem des Empfängers derart entschlüsselt vorliegen, daß die Weiterverbreitung der entschlüsselten Daten nicht kontrollierbar ist.

Es ist die Aufgabe der vorliegenden Erfindung, ein Computersystem und ein Verfahren zur Ausgabe von verschlüsselten Daten so auszubilden, daß verschlüsselte von einem Netzwerk übermittelte Daten von dem Computersystem genutzt werden können, die Weiterverbreitung der unverschlüsselten Daten jedoch erschwert wird.

Diese Aufgabe wird durch die Merkmale des Patentanspruches 1 bzw. des Patentanspruches 7 gelöst, wobei sich weitere Ausgestaltungen aus den Unteransprüchen ergeben.

Kern der Erfindung ist, daß die verschlüsselten Informationen durch eine Verschlüsselungseinheit so für die Ausgabe durch die Ausgabeeinheit entschlüsselt werden, daß die unverschlüsselten Daten nicht unmittelbar digital weiterverarbeitet oder gespeichert werden können.

Die Entschlüsselung geschieht also nicht durch ein auf dem Zentralprozessor ablaufendes Programm, sondern erst in oder unmittelbar vor der Ausgabeeinheit, also z. B. dem Drucker bzw. der Grafikkarte. Die entschlüsselten Daten liegen nicht in digitaler, unmittelbar elektronisch weiterverbreitbarer Form vor. Dies ist im Sinne des Informationslieferanten, der an der Nutzung durch den Empfänger interessiert ist, eine digitale Weiterverbreitung jedoch ausschließen möchte. Dadurch wird eine Äquivalenz z. B. zum Papierdruck erreicht, bei dem die Daten unmittelbar genutzt, also gelesen werden können, jedoch nicht ohne erheblichen Aufwand weiterverbreitbar sind.

Das erfindungsgemäße Computersystem zeichnet sich dadurch aus, daß zwischen der Zentraleinheit und der Ausgabeeinheit eine Entschlüsselungseinheit vorgesehen ist, welche die von der Zentraleinheit kommenden Daten entschlüsselt und welche die entschlüsselten Daten nur an die für die Ausgabe von unverschlüsselten Daten vorgesehene/n Ausgabeeinheit/en übermittelt, wobei in dem Computersystem keine Mittel zur Übermittlung der entschlüsselten Daten zurück an die Zentraleinheit oder an eine andere Einheit des Computersystems vorgesehen sind. Vorteilhaft an dem erfindungsgemäßen Computersystem ist, daß die verschlüsselten Daten nur für bestimmte vorbestimmte Ausgabeeinheiten des Computersystems entschlüsselt werden, so daß diese Daten nur über diese Ausgabeeinheiten genutzt werden können. Eine Übermittlung der entschlüsselten Daten an beispielsweise eine Ausgabeschnittstelle oder eine Speichereinheit des Computersystems ist bei dem erfindungsgemäßen Computersystem nicht möglich, so daß die unverschlüsselten Daten über diese Ausgabeeinheiten nicht weiterverbreitet werden können.

In einer Ausbildung der Erfindung entschlüsselt die

Entschlüsselungseinheit des Computersystems Daten, die mittels eines asymmetrischen Verschlüsselungsverfahrens oder mittels eines Public-Private-Key-Verfahrens verschlüsselt worden sind. Vorteilhaft an derart verschlüsselten Daten ist, daß sie gegen eine Entschlüsselung von Unberechtigten sicher sind.

Die Ausgabeeinheit des erfindungsgemäßen Computersystems, für die die verschlüsselten Daten durch die Entschlüsselungseinheit entschlüsselt werden, kann beispielsweise der Bildschirm oder der Drucker des Computersystems sein. Dies ist vorteilhaft, weil dadurch die unverschlüsselten Daten höchstens als Bildschirminformation oder Druckerinformation vorliegen und somit eine unproblematische Weiterverbreitung nicht möglich ist.

In einer weiteren Ausgestaltung des Computersystems ist die Ausgabeeinheit getrennt von der Zentraleinheit vorgesehen, wobei die Entschlüsselungseinheit in die Ausgabeeinheit integriert ist. Vorteilhaft an dieser Ausbildung ist, daß nur bestimmte Ausgabeeinheiten, wie z. B. der Drucker oder die Grafikkarte bzw. der Bildschirm eines Computersystems, mit der Entschlüsselungseinheit versehen werden können.

In einer weiteren Ausbildung des erfindungsgemäßen Computersystems ist der private Schlüssel der Entschlüsselungseinheit, welcher zur Entschlüsselung von mit dem öffentlichen Schlüssel der Entschlüsselungseinheit verschlüsselten Daten dient, geheim in der Entschlüsselungseinheit vorgesehen. Vorteilhaft an dieser Ausbildung ist, daß, selbst wenn der Benutzer des Computersystems sich Zugang zu den verschlüsselten Daten verschaffen würde, ihm der private Schlüssel, durch den er die verschlüsselten Daten entschlüsseln könnte, nicht bekannt ist.

Bei dem erfindungsgemäßen Verfahren zur Ausgabe von verschlüsselten Daten werden die verschlüsselten Daten über eine Schnittstelle empfangen und an eine Zentraleinheit übermittelt. Daraufhin werden die verschlüsselten Daten für die Ausgabe von der Zentraleinheit an eine Entschlüsselungseinheit übermittelt und von dieser entschlüsselt. Die entschlüsselten Daten werden von der Entschlüsselungseinheit an eine bestimmte, zur Ausgabe von unverschlüsselten Daten vorgesehene Ausgabeeinheit übermittelt und von dieser ausgegeben. Dabei ist es bei dem erfindungsgemäßen Verfahren nicht möglich, daß die entschlüsselten Daten zurück an die Zentraleinheit oder an eine andere Einheit des Computersystems, von der die unverschlüsselten Daten nicht weiterverarbeitet werden sollen (z. B. eine Speichereinheit), übermittelt werden. Vorteilhaft an dem erfindungsgemäßen Verfahren ist, daß die verschlüsselten beispielsweise von einem Netzwerk übermittelten Daten zwar vom Empfänger genutzt, d. h. beispielsweise ausgedruckt oder angezeigt, werden können, eine Weiterverbreitung der unverschlüsselten Daten auf elektronischem Weg jedoch nicht möglich ist.

Die vorliegende Erfindung wird nun anhand von Ausführungsbeispielen mit Bezug zu der einzigen Figur erläutert. Diese zeigt das erfindungsgemäße Computersystem schematisch.

Das erfindungsgemäße Computersystem 1 weist eine Schnittstelle 3 auf, die verschlüsselte Informationen I_V von einem Computernetzwerk 2 erhält. Ferner ist der Empfang der verschlüsselten Daten auch über andere Informationsmedien möglich. So könnte beispielsweise die Einheit 2 auch eine Diskette oder ähnliches darstellen, wobei mit dem Bezugszeichen 3 dann die entsprechende Ableseeinheit des Computersystems bezeichnet wäre. Die verschlüsselten Daten I_V, die von der Schnittstelle 3 empfangen worden sind, werden von dieser an die Zentraleinheit 4 des Computersystems übermittelt. Wesentlich an dem erfindungsgemäßen Computersystem ist, daß die Informationen I in der Zentraleinheit 4 immer in verschlüsselter Form vorliegen. Soll beispielsweise die Information I wieder über das Netzwerk 2 weiterverbreitet werden, kann dies nur mit der verschlüsselten Information I_V erfolgen. Auch erfolgt die Verarbeitung der Information in der Zentraleinheit 4 im verschlüsselten Zustand. Zur Nutzung der Information muß diese nun dem Benutzer des Computersystems 1 zugänglich gemacht werden. Hierzu sind für das Computersystem 1 Ausgabeeinheiten 6, 7, 8 vorgesehen. Dabei stellt bei dem in der Figur dargestellten Beispiel die Ausgabeeinheit 6 eine Speichereinheit, wie z. B. ein Diskettenlaufwerk, dar, die Ausgabeeinheit 7 einen Bildschirm und die Ausgabeeinheit 8 einen Drucker dar. Soll die Information auf dem Bildschirm 7 dem Benutzer des Computersystems 1 dargestellt werden, übermittelt die Zentraleinheit 4 die verschlüsselte Information I_V an eine Entschlüsselungseinheit 5. Die Entschlüsselungseinheit 5 entschlüsselt die Information und übermittelt die unverschlüsselte Information I_U an den Bildschirm 7. Wesentlich an dem erfindungsgemäßen Computersystem 1 ist dabei, daß von der Entschlüsselungseinheit 5 die unverschlüsselte Information nur an eine bestimmte erwünschte Ausgabeeinheit übermittelt werden kann. Soll gleichfalls zur Nutzung die Information auf einem Drucker ausgegeben werden, übermittelt die Zentraleinheit 4 die verschlüsselte Information I_V an eine weitere Entschlüsselungseinheit 5, die nach der Entschlüsselung der Information diese an den Drucker 8 übermittelt. Anstatt wie in der Figur dargestellt zwei Entschlüsselungseinheiten 5 für die Ausgabe auf die Ausgabeeinheit 7 bzw. die Ausgabeeinheit 8 vorzusehen, wäre es auch möglich, nur eine Entschlüsselungseinheit 5 vorzusehen, die die unverschlüsselte Information I_U entweder an die Ausgabeeinheit 7 oder die Ausgabeeinheit 8 übermitteln kann.

In dem hier erläuterten Ausführungsbeispiel sind die Informationen, die über die Schnittstelle 3 von dem Computersystem 1 empfangen werden, mittels eines Public-Private-Key-Verfahrens verschlüsselt worden. Hierzu wurde die Information I vom Sender vor dem Versand mittels des öffentlichen Schlüssels KÖ der Entschlüsselungseinheit 5 verschlüsselt. Der private Schlüssel KP der Entschlüsselungseinheit 5 ist nicht zugänglich von der Entschlüsselungseinheit 5 gespeichert. Somit ist die einzige Möglichkeit, die verschlüsselte Information I_V zu entschlüsseln, diese in die Entschlüsselungseinheit 5 einzuspeisen. In der Entschlüsselungseinheit 5 wird die verschlüsselte Information I_V mittels des privaten Schlüssels KP der Entschlüsselungseinheit 5 entschlüsselt. Da nun das erfindungsgemäße Computersystem 1 so ausgebildet ist, daß die Daten, die von der Entschlüsselungseinheit 5 entschlüsselt worden sind, nur an bestimmte, für die Ausgabe von unverschlüsselten Daten bestimmte Ausgabeeinheiten geliefert werden, ist eine unerwünschte Weiterverbreitung der unverschlüsselten Daten nicht möglich. Um die unerwünschte Weiterverbreitung noch weiter zu erschweren, wäre es möglich, daß die Entschlüsselungseinheit 5, die beispielsweise für einen Drucker als Ausgabeeinheit 8 vorgesehen ist, die unverschlüsselte Information als Pixelwerte für den Drucker ausgibt.

Es sei bemerkt, daß der Begriff "Computersystem" gemäß der hier vorliegenden Erfindung in einem sehr

weiten Sinn zu verstehen ist. So kann das Computersystem ein Drucker sein, der eine zentrale Verarbeitungseinheit 4, eine Schnittstelle 3 zum Empfang der zu drukkenden Daten, beispielsweise von einem Personal Computer (PC), und als Ausgabeeinheit 7 die Druckertrommel aufweist. In diesem Fall ist die Entschlüsselungseinheit zwischen der zentralen Verarbeitungseinheit 4 des Druckers und der Druckertrommel 7 vorgesehen. Ferner könnte das Computersystem eine Einsteckkarte für einen PC sein, z. B. eine Grafikkarte, deren Schnittstelle 3 die Steckverbindung ist, über die Daten von der CPU des PCs kommen, deren Zentraleinheit 4 ein bestimmter elektronischer Teil auf der Karte ist, und deren Ausgabeeinheit 7 der Stecker für das Monitorkabel ist. In diesem Fall ist die Entschlüsselungseinheit 5 zwischen der zentralen Elektronik 4 der Steckkarte und dem Monitorkabel-Stecker 7 vorgesehen.

Im folgenden wird eine mögliche Ausführung der Erfindung in Form eines Beispieles beschrieben.

Informationslieferant ist eine Zeitung Z, die einem Leser L von diesem bestellte Informationen I, z. B. speziell abonnierte Zeitungsseiten, über das Internet liefern möchte. Die Zeitung Z ist daran interessiert, daß der Leser L die Information I lesen kann, möchte jedoch verhindern, daß die Informationen I vom Leser L in digitaler Form weiterverbreitet werden. Der Leser L soll die Information I an seinem Bildschirm lesen oder auf seinem Drucker ausdrucken, nicht jedoch unverschlüsselt speichern oder in für Dritte nutzbarer Form weiterversenden können. Die Übertragung der Informationen soll über einen öffentlichen, nicht abhörsicheren Kanal möglich sein. Zunächst fordert daher der Leser L von der Zeitung Z die Information I an. Die Zeitung möchte sicherstellen, daß die Information I nur vom Drucker D des Lesers L, nicht jedoch von dessen Computer selbst entschlüsselt werden kann. Deshalb liefert der Leser L bei der Anforderung der Information den öffentlichen Schlüssel KÖD seines Druckers D mit, der z. B. als vierzigstellige Zahlenkombination auf dem Gehäuse des Druckers aufgedruckt ist. Der private Schlüssel KPD des Druckers D ist dem Leser L nicht bekannt, sondern in die Druckerelektronik integriert. Die Zeitung erstellt die gewünschten Zeitungsseiten (I), verschlüsselt diese mit dem Schlüssel KÖD zu einem Datenstrom IV und sendet diesen per E-Mail an den Leser L. Dieser sendet den verschlüsselten Datenstrom IV an seinen Drucker D. Im Drucker D wird der Datenstrom IV mit dem privaten Schlüssel KPD des Druckers entschlüsselt und die gewünschten Zeitungsseiten in lesbarer Form I ausgedruckt. Eine analoge Anwendung ist denkbar für die Lieferung am Bildschirm dargestellter Grafikseiten über das Word Wide Web. Die Entschlüsselung würde in diesem Fall erst in der Grafik-Controller-Karte und noch nicht im Zentralprozessor des Computers erfolgen. Der Lieferant der Information könnte hier z. B. daran interessiert sein, daß die Informationen nur gelesen, nicht jedoch gedruckt werden können.

Ein zusätzliches Problem ist zu lösen: Die Zeitung Z muß sicherstellen können, daß der gelieferte öffentliche Schlüssel KÖD des angeblichen Druckers tatsächlich ein gültiger öffentlicher Schlüssel z. B. eines Druckers der Marke X ist und nicht ein vom Leser L selbst generierter öffentlicher Schlüssel, zu dem dieser den passenden privaten Schlüssel besäße. Diese Verifikation leistet die nochmalige Anwendung des Public/Private-Key-Vefahrens auf die Schlüssel selbst. Auf dem Drucker ist dazu nicht der eigentliche öffentliche Schlüssel KÖD des Druckers selbst aufgedruckt, sondern vielmehr der mit dem privaten Schlüssel KPX des Druckerherstellers X verschlüsselte öffentliche Schlüssel KÖD des speziellen Druckerexemplars D, hier KÖDX genannt. Diese Zahlenkombination KÖDX wird an die Zeitung geliefert. Die Zeitung entschlüsselt die Zahlenkombination zunächst mit dem bekannten öffentlichen Schlüssel KÖX des Druckerherstellers X und erhält damit den garantiert ungefälschten öffentlichen Schlüssel KÖD des speziellen Druckerexemplars D, mit dem dann wiederum die Information I vor dem Versand verschlüsselt wird. Wenn die vom Leser L gelieferte Zahlenkombination KÖDX gefälscht ist, führt die Entschlüsselung mit dem öffentlichen Schlüssel KÖX des Druckerherstellers X durch die Zeitung zu einem ungültigen öffentlichen Schlüssel KÖD des speziellen Druckerexemplars D.

Dieses Verfikationsverfahren ist Stand der Technik und in verschiedenen Publikationen beschrieben. Die Funktion der dort beschriebenen Verifikationsinstanz oder Autorisierungsbehörde übernimmt in dem hier vorgestellten Beispiel der Druckerhersteller X.

Patentansprüche

1. Computersystem (1) mit
   - einer Schnittstelle (3) zum Empfang von verschlüsselten Daten,
   - mindestens einer Ausgabeeinheit (7, 8) zur Ausgabe von unverschlüsselten Daten und
   - einer Zentraleinheit (4) zum Empfang der Daten von der Schnittstelle (3) und zur Übermittlung auszugebender Daten an eine Ausgabeeinheit (7, 8),

   dadurch gekennzeichnet,

   daß zwischen der Zentraleinheit (4) und der Ausgabeeinheit (7, 8) eine Entschlüsselungseinheit (5) vorgesehen ist, welche die von der Zentraleinheit (4) kommenden Daten entschlüsselt und welche die entschlüsselten Daten nur an die zur Ausgabe von unverschlüsselten Daten vorgesehene/n Ausgabeeinheit/en (7, 8) übermittelt, wobei in dem Computersystem (1) keine Mittel zur Übermittlung der entschlüsselten Daten zurück an die Zentraleinheit (4) vorgesehen sind.

2. Computersystem (1) nach Anspruch 1, dadurch gekennzeichnet, daß die Entschlüsselungseinheit (5) Daten entschlüsselt, die mittels eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt worden sind.

3. Computersystem (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Entschlüsselungseinheit (5) Daten entschlüsselt, die mittels eines Public-Private-Key-Verfahrens verschlüsselt worden sind.

4. Computersystem (1) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Ausgabeeinheit (7, 8) ein Bildschirm und/oder ein Drucker ist.

5. Computersystem (1) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Ausgabeeinheit (7, 8) getrennt von der Zentraleinheit (4) vorgesehen ist und daß die Entschlüsselungseinheit (5) in die Ausgabeeinheit (7, 8) integriert ist.

5. Computersystem (1) nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, daß der private Schlüssel der Entschlüsselungseinheit (5), der zur Entschlüsselung von mit dem öffentlichen Schlüssel der Entschlüsselungseinheit (5) verschlüsselten Da-

ten dient, geheim in der Entschlüsselungseinheit (5) vorgesehen ist.

7. Verfahren zur Ausgabe von verschlüsselten Daten, bei dem

— die verschlüsselten Daten über eine Schnittstelle (3) empfangen werden,

— die verschlüsselten Daten an eine Zentraleinheit (4) übermittelt werden und

— die entschlüsselten Daten von einer Ausgabeeinheit (7, 8) ausgegeben werden,

dadurch gekennzeichnet,

— daß die verschlüsselten Daten für die Ausgabe von der Zentraleinheit (4) an eine Entschlüsselungseinheit (5) übermittelt werden,

— daß die verschlüsselten Daten von der Entschlüsselungseinheit (5) entschlüsselt werden und

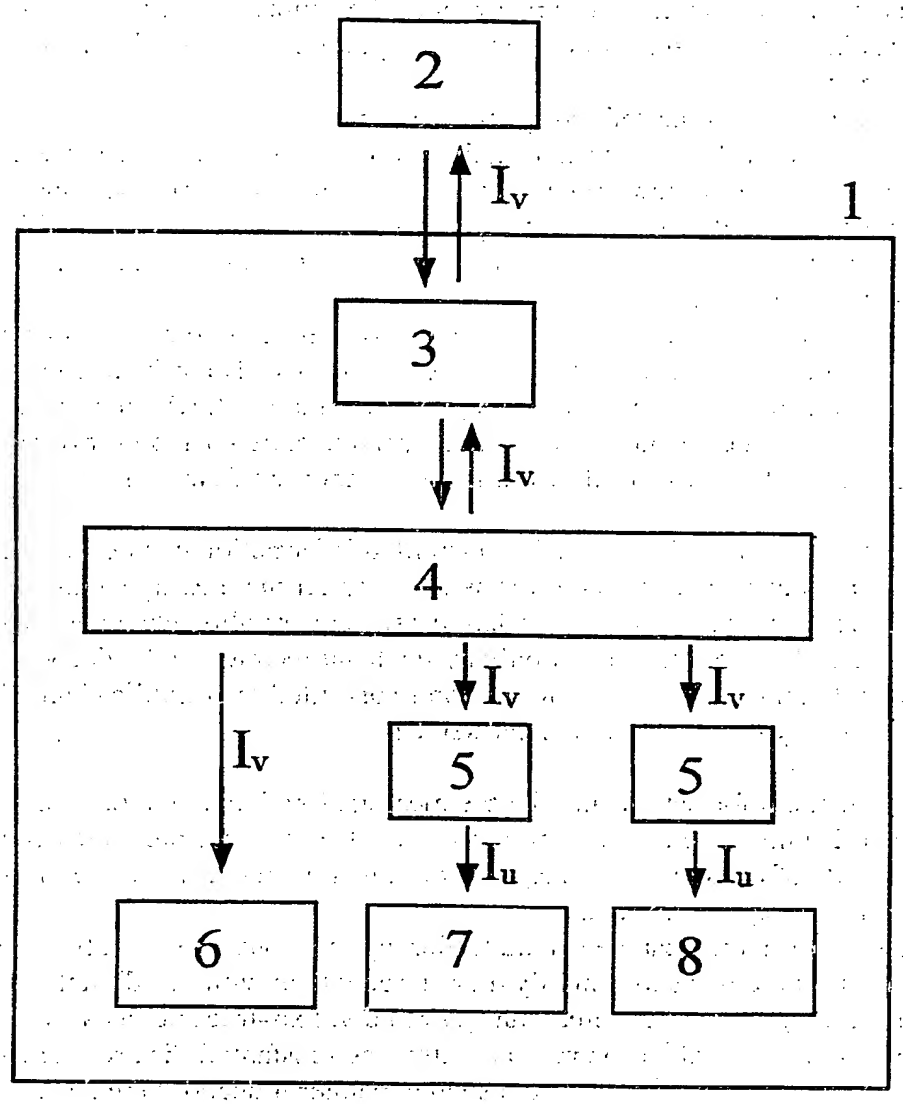
— daß die entschlüsselten Daten von der Entschlüsselungseinheit (5) an die zur Ausgabe von unverschlüsselten Daten vorgesehene Ausgabeeinheit (7, 8) übermittelt werden,

wobei die entschlüsselten Daten nicht zurück an die Zentraleinheit (4) übermittelt werden.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 38 623 A1
Int. Cl.[6]: H 04 L 9/30
Offenlegungstag: 26. März 1998

Fig.



The available invention refers to a computer system with an interface to the reception of encoded data, at least one output unit to the output of unencrypted data and a central processing unit for the reception of the data of the interface and for the transmittal of data which can be output to an output unit after the header of the patent claim 1.
Furthermore the invention refers to a procedure for the output by encoded data, with which the encoded data will receive over an interface, the encoded data to a central processing unit to be transmitted and the decoded data by an output unit be output after the header of the patent claim 7.
In networks individual computer systems are connected, which send themselves mutually encoded data. As example of such a network the Internet is to be called. There information and audiovisual signals are spread. The majority of the supply are free information. Monetary values information are offered so far hardly, but remain beschrankt on conventional distribution channels.
This has among other things the following three reasons:
First of all procedures for the comfortable zahlungsabwicklung are so far not yet common. Secondly there are so far only few procedures for the secured information transfer. Safe procedures are predominantly based on cryptographic publication IC/PRIVATE key procedures. These procedures are distinguished by the fact that each user in information exchange possesses two codes:
A public code KÖ and a private code kp. A connection between both is not derivable. The public code of each user can be taken from public directories. The private code remains secret and is only for the user himself well-known. Information I, which was encoded with the public code KÖ, can be decoded only with the private code kp and in reverse.
Publication IC/PRIVATE key procedures fulfill two important functions:

a) you guarantee that over public channels transmitted information can be used only by the legal recipient. In addition encode the information supplier the message with the public code of the legal recipient and dispatch the encoded message over public channels. This encoded message can receive from everyone, but only by the legal recipient to be decoded and used.
b) you guarantee that the recipient of information transmitted over public channels can go surely that this actually comes from the legal sender.

In addition encode the information supplier the message I with his own private code and dispatch the encoded message I over public channels. If with a recipient the decoding attempt with the public code of the supplier Z succeeds to L, this guarantees that the message I also really comes from the legal supplier Z.
Thirdly available information can be spread further by this abusively with the recipient in digital form. This problem is substantially more largely than with not-digital carrier media (e.g. paper), there a digital further spread further rapidly, loss-free and cheaply possible is.
In accordance with latter third reason results in itself as substantial disadvantage conventional information spreading over networks that in such a manner it decodes the data, if they are even transmitted encoded in the computer system of the recipient, provided over the network, to be present that the further spread of the decoded data further is not controllable.
It is the function of the available invention in such a way to train a computer system and a procedure for the output of encoded data that encoded by a network transmitted data by the computer system be used can, which further spread of the unencrypted data further is however made more difficult.
This function is solved by the features of the patent claim 1 or the patent claim 7, whereby

further arrangements result from the unteranspruechen.
Core of the invention is that the encoded information is decoded in such a way by an encoding unit for the output by the output unit that the unencrypted data cannot be continued to process or stored directly digitally.
The decoding is done thus not via a program, but only in or directly before the output unit, running on the master processor, thus e.g. the printer or the diagram card. The decoded data are not present in digital, directly electronically widespreadweiterverbreitbarer form. This is in the sense of the information supplier, who is interested by the recipient in the use, a digital further spread further however to exclude would like. Thus an equivalence e.g. to the paper printing achieved, with which the data can be used directly, read thus, however not without substantial expenditure widespreadable are.
The computer system according to invention is distinguished by the fact that between the central processing unit and the output unit a decoding unit is intended, which the data coming from the central processing unit decoded and which transmits the decoded data only to for the output of unencrypted data vorgesehene/n the Ausgabeeinheit/en, whereby in the computer system no means are intended for the transmittal of the decoded data back to the central processing unit or to another unit of the computer system. At the computer system according to invention it is favourable that the encoded data are decoded only for certain pre-determined output units of the computer system, so that these data are not used only over these output units ability one transmittal of the decoded data to for example an output interface or a memory unit of the computer system are with the computer system according to invention possible, so that the unencrypted data cannot be spread further over these output units.
In a formation of the invention the decoding unit of the computer system decodes data, which were encoded by means of an asymmetrical encoding procedure or by means of a publication IC private key procedure. At in such a manner encoded data it is favourable that they are safe against a decoding of unauthorized ones.
The output unit of the computer system according to invention, for which the encoded data are decoded by the decoding unit, can be for example the display or the printer of the computer system. This is favourable, because thereby the unencrypted data are present at the most as display information or printer information and are not possible thus an unproblematic further spread further.
In a further arrangement of the computer system the output unit is separately from the central processing unit intended, whereby the decoding unit is integrated into the output unit. At this formation it is favourable that only determined output units, e.g. the printer or the diagram card or. the display of a computer system, with which will provide decoding unit can.
In a further formation of the invention-in accordance with-eaten computer system the private code of the decoding unit, which serves the decoding unit for the decoding of with the public code data encoded, is secretly in the decoding unit intended. Favourable to this formation is that, if the user of the computer system would even provide receipt to the encoded data the private code, by which it could decode the encoded data does not admit to it is.
With the procedure according to invention for the output of encoded data the encoded data will receive over an interface and transmitted to a central processing unit. Thereupon the encoded data for the output are transmitted by the central processing unit to a decoding unit and decoded by this. The decoded data are transmitted by the decoding unit to a certain output unit designated to the output of unencrypted data and output by this. It is not possible with the procedure according to invention that the decoded data back to the central processing unit or to another unit of the computer system, by which the unencrypted data (e.g. a memory unit) are not to be continued to process, at the procedure according to invention are

transmitted will favourable that the encoded for example data transmitted by a network used by the recipient, i.e. for example printed out or displayed, to become to be able, a further spread of the unencrypted data further on electronic way is however not possible.
The available invention is described now on the basis of execution examples with reference to the only figure. This shows the computer system according to invention schematically.
The computer system according to invention 1 indicates an interface 3, which receives encoded information Iv from a computer network 2. Furthermore the reception of the encoded data is possible also over other information media. So for example the unit 2 could represent also a diskette or a like, whereby the reference symbol 3 then the appropriate reading off unit of the computer system would be named. The encoded data Iv, which were received from the interface 3, are transmitted by this to the central processing unit 4 of the computer system. At the invention-in accordance with-eaten computer system it is substantial that the information I in the central processing unit 4 is always present in encoded form. For example if the information I is to be spread further again over the network 2, this can take place only with the encoded information Iv. Also the processing of the information takes place in the central processing unit 4 in the encoded status. The use of the information this must be made accessible now for the user of the computer system 1. For this output units 6, 7, 8 are intended for the computer system 1. The output unit 6 places a memory unit with the example represented in the figure, e.g. a floppy disk drive, the output unit 7 a display and the output unit 8 a printer. If the information on the display 7 is to be represented to the user of the computer system 1, the central processing unit 4 transmits the encoded information Iv to a decoding unit 5. The decoding unit 5 decodes the information and transmits the unencrypted information Iu to the display 7. At the computer system according to invention 1 it participates substantial that by the decoding unit 5 the unencrypted information can be transmitted only to a certain desired output unit. If the information on a printer is to be also output for use, the central processing unit 4 transmits the encoded information Iv to a further decoding unit 5, which transmits these after the decoding of the information to the printer 8. Instead of designating as in the figure represented two decoding units 5 for the output on the output unit 7 or the output unit 8, it would be also possible to designate only one decoding unit 5 which can transmit the unencrypted information Iu either to the output unit 7 or the output unit 8.
In the execution example described here the information, which will receive 3 from the computer system 1 over the interface, was encoded by means of a publication IC of private key procedure. For this the information I was encoded by the sender before the dispatch by means of the public code KÖ of the decoding unit 5. The private code kp of the decoding unit 5 is not accessible stored of the decoding unit 5. Thus the only possibility is of decoding the encoded information Iv of feeding these into the decoding unit 5. In the decoding unit 5 the encoded information Iv is decoded by means of the private code kp of the decoding unit 5. Since now the computer system according to invention 1 is so trained that the data, which were decoded by the decoding unit 5 only at certain for which output by unencrypted data determined output units are supplied, it is not possible an unwanted further spread of the unencrypted data further. In order to make unwanted further spread further more difficult still further, it would be possible that the decoding unit 5, which is intended for example for a printer as output unit 8, which outputs unencrypted information as pixel values on the printer. It is noticed that the term is to be understood " computer system " in accordance with the here available invention in a very broad sense. So the computer system can be a printer, the one central processing unit 4, an interface 3 for the reception of the data which can be printed, for example by a personnel computer (PC), and as output unit 7 the printer drum indicates. In

this case the decoding unit between the central processing unit 4 of the printer and the printer drum 7 is intended. Furthermore the computer system could be a plugging in card for a PC, come e.g. a diagram card, whose interface 3 is the patch cord, over the data of the CCU of the PC, whose central processing unit 4 is a certain electronic section on the card, and whose output unit 7 is the plug for the monitor cable ist.In this case the decoding unit 5 between central electronics 4 of the plug-in card and the monitor connector 7 intended.
In the following a possible execution of the invention in form of an example is described. Information supplier is a newspaper Z, which subscribed a reader L of this ordered information I, e.g. particularly zeitungsseiten, over which Internet would like to supply. The newspaper Z is interested in it that the reader L can read the information I, would like however to prevent that the information I is spread further by the reader L in digital form. The reader L is to read the information I at its display or on its printer printouts, however unencrypted not store or in form usable for third to further-dispatch be able. The transfer of the information should be possible over a public, not hear-safe channel. First therefore the reader L of the newspaper Z calls the information I. The newspaper would like to guarantee that the information I can be decoded only by the printer D of the reader L, not however of its computers themselves. Therefore the reader L provides the public code KÖD of its printer D, which is imprinted e.g. as forty-digit number combination on the housing of the printer during the request of the information. The private code KPD of the printer D is not well-known the reader L, but integrates into printer electronics. The newspaper creates the desired zeitungsseiten (I), encodes these with the key KÖD to a data stream IV and transmits these by E-Mail to the reader L of these transmits the encoded data stream IV to its printer D. in the printer D the data stream IV with the private code KPD of the printer is decoded and the desired zeitungsseiten in readable form I printed out. A similar application is conceivablly for the supply at the display of represented diagram pages over the Word Wide Web.Die decoding in this case only in the diagram CONTROLLER card and yet in the master processor of the computer would not take place. The supplier of the information could be interested e.g. in the fact here that the information only read, not however to be printed to be able.
An additional problem is to be solved: The newspaper Z must be able to guarantee that the supplied public code KÖD of the alleged printer is actually a valid public code e.g. a printer of the label X and not a public code generated by the reader L itself, to which this would possess the suitable private code. This verification carries the repeated application out of the Public/Private key Vefahrens to the codes themselves. On the printer in addition the actual public code KÖD of the printer itself is not imprinted, but rather with the private code KPX of the printer manufacturer X encoded public codes KÖD of the special printer copy D, here KÖDX mentioned. This number combination KÖDX is supplied to the newspaper. The newspaper decodes the number combination first with the well-known public code KÖX of the printer manufacturer X and receives thereby guarantees genuine public code KÖD of the special printer copy D, with which then again the information I before the dispatch is encoded. If the number combination KÖDX supplied by the reader L is falsified, the decoding with the public code KÖX of the printer manufacturer X leads by the newspaper to an invalid public code KÖD of the special printer copy D.
This Verfikationsverfahren is described state of the art and in different publications. The function of the verification instance or authorizing authority described there transfers in the example of the printer manufacturers X presented here.

1. Computer system (1) also

- an interface (3) to the reception of encoded data,
- at least one output unit (7, 8) to the output of unencrypted data and
- a central processing unit (4) for the reception of the data of the interface (3) and for the transmittal of data to an output unit (7, 8), which can be output,

thus characterized,
the fact that between the central processing unit (4) and the output unit (7, 8) a decoding unit (5) is intended, which the data coming from the central processing unit (4) decoded and which transmits the decoded data only to to the output of unencrypted data vorgesehene/n the Ausgabeeinheit/en (7, 8), whereby in the computer system (1) no means are intended for the transmittal of the decoded data back to the central processing unit (4).
2.Computersystem (1) according to demand 1, by the fact characterized that the decoding unit decodes (5) data, which were encoded by means of an asymmetrical encoding procedure.
3. Computer system (1) according to demand 1 or 2, by the fact characterized that the decoding unit decodes (5) data, which were encoded by means of a publication IC private key of procedure.
4. Computer system (1) after one of the preceding demands, by the fact characterized that the output unit (7, 8) is a display and/or a printer.
5. Computer system (1) after one of the preceding demands, by the fact characterized that the output unit (7, 8) is intended separately from the central processing unit (4) and that the decoding unit (5) is integrated into the output unit (7, 8).
5.Computersystem (1) after one of the demands 3 to 5, by the fact characterized that the private code of the decoding unit (5), which for the decoding of data encoded with the public code the decoding unit (5) serves is secretly in the decoding unit (5) intended.
7. Procedure for the output of encoded data, with that

- the encoded data over an interface (3) to be received,
- the encoded data to a central processing unit (4) to be transmitted and
- the decoded data by an output unit (7, 8) to be output,

thus characterized,

- that the encoded data for the output are transmitted by the central processing unit (4) to a decoding unit (5),
- that the encoded data are decoded by the decoding unit (5) and
- that the decoded data are transmitted by the decoding unit (5) to the output unit designated to the output of unencrypted data (7, 8),

whereby the decoded data back to the central processing unit (4) to be transmitted.